#5

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

ATTORNEY DOCKET NO. 058856-0109

Applicant: Yasumasa UYAMA

Title: PROTECTED COMMUNICATION SYSTEM

Appl. No.: 10/021,052

Filing Date: 12/19/2001

Examiner: Unassigned

Art Unit: 2131

CLAIM FOR CONVENTION PRIORITY

Commissioner for Patents
Washington, D.C. 20231

Sir:

The benefit of the filing dates of the following prior foreign applications filed in the following foreign country is hereby requested, and the right of priority provided in 35 U.S.C. § 119 is hereby claimed.

In support of this claim, filed herewith are certified copies of said original foreign applications:

Japanese Patent Application No. 2000-388921 filed December 21, 2000
Japanese Patent Application No. 2001-326908 filed October 24, 2001
Japanese Patent Application No. 2001-370959 filed December 5, 2001

Respectfully submitted,

March 15, 2002
Date

William T. Ellis
Attorney for Applicant
Registration No. 26,874

FOLEY & LARDNER
Customer Number: 22428
22428
PATENT TRADEMARK OFFICE
Telephone: (202) 672-5485
Facsimile: (202) 672-5399

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２０００年１２月２１日

出願番号
Application Number: 特願２０００－３８８９２１

ST.10/C]: [ＪＰ２０００－３８８９２１]

出願人
Applicant(s): 宇山　靖政

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００２年　１月１１日

特許庁長官
Commissioner,
Japan Patent Office 及川耕造

出証番号　出証特２００１－３１１３１６６

【書類名】　特許願

【整理番号】　YU2000-01

【あて先】　特許庁長官　殿

【国際特許分類】　H04K　1/00

【発明者】

【住所又は居所】　神奈川県横須賀市久里浜　８－３０－１５－５０４

【氏名】　宇山　靖政

【特許出願人】

【識別番号】　300085864

【氏名又は名称】　宇山　靖政

【手数料の表示】

【予納台帳番号】　123963

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　　順序対方式暗号通信

【特許請求の範囲】

【請求項１】　記憶装置と演算装置を利用できる情報機器による暗号を利用した秘密通信の方法のうちで、送信者（Ｓ）と受信者（Ｒ）の順序対（Ｓ，Ｒ）に対して一意的に決まる暗号化方式（Ｃsr）と復号化方式（Ｐsr）に従って暗号を利用した通信を自動的に行うもので、順序対（Ｓ，Ｒ）に対応する暗号化方式を受信者（Ｒ）が前もって自由に指定しておくことができる秘密通信の方法。

【請求項２】　暗号化の指定欄と復号化の指定欄がある識別記号（メールアドレスや電話番号）一覧を備え、送信時には情報の受信者が前もって指定した方式により自動的に暗号化を行い、受信時には送信者に対応する復号化方式により自動的に復号化することで、請求項１の秘密通信の方法を実現する通信用ソフトウエア。

【請求項３】　暗号ソフトの形式のうち、暗号化部分と復号化部分に分割でき、暗号化部分の自由な再配布を認めるが、復号化部分の自由な再配布は認めない形式。

【請求項４】　有料での情報配信の方法で、上記の請求項１，２，３の利用によって少なくとも顧客の要求する以上の強度を持つ暗号化によって情報を配信する方法。

【発明の詳細な説明】

【０００１】

【発明が属する技術分野】

本発明は、ネットワーク上での秘密通信を実施する方法に関するものである。

【０００２】

【従来の技術】

情報通信の安全性を確保する技術として、送信する情報を暗号化して送る方法があるが、それには面倒な手順が必要である。また、暗号の解読技術の進歩に合わせて、新しい強力な暗号方式を手軽に利用することは困難な状況にある。

【０００３】

【この発明が解決しようとする課題】

安全で信頼性のある情報通信を簡単に、自動的に行える状況ではなく、多くの人がネットワーク社会に対し不安感を持ち、積極的に参加することにとまどいを持っている。誰もが安心して気軽にネットワーク社会に参加できるようにしなくてはならない。

【０００４】

【発明の目的】

本発明の目的は秘密通信の方法を改善し、誰もが簡単に暗号技術を利用できるようにすること、暗号解読の技術の発展を考慮して新しい暗号化方式に切り替えることが簡単に行えるようにすることである。

【０００５】

【課題を解決するための手段】

送信者と受信者の順序対に対して、暗号化方式と復号化方式を一意的に決定し、この方式に従った暗号通信が行われるように通信用ソフトの機能を拡張する。暗号方式の指定欄を持つアドレス帳を利用して、暗号化や復号化が自動的に行えるようにする。

暗号解読技術の発展に合わせて新しい暗号方式に簡単に変更できるような方法を実現する。そして情報の受信者が暗号方式を自由に決定できるようにする。

暗号ソフトの構造を、暗号化部分と復号化部分の二つにわけ、暗号化部分の自由な再配布を認めるようにする。また、復号化部分の再配布を禁止できるようにしておく。これによって、暗号ソフトを商業ベースで開発販売する事を経済的に保証でき、優れた暗号ソフトが安定して供給されるようになる。

この方式は電話による通信の場合でも利用できるが、現在の電話機に記憶装置と演算装置を付け加える必要がある。さらに、いくつかの項目について規格を統一する必要がある。

そこで、現在のハードウエアですぐに実現できるインターネットの電子メールに関する事柄を中心に記述する事にする。

【０００６】

【この発明で利用される自然法則】

２つのもの　X、Y　に順序を付けて並べる方法は（X、Y）と（Y、X）の２種類であり、これ以外にはない。という自然法則を利用してこの発明を実現する。

【０００７】

【発明の実施の形態】

【０００８】

【アドレスの一意性とその順序対】

インターネット社会ではメールアドレスやIPアドレスなど個人を特定するための識別記号が存在する。情報の発信者と受信者の２者を特定すれば、二つのメールアドレスから（発信者、受信者）の順序対を決定できる。

この順序対に対応して暗号化方式を決定できるような仕組みを作る。（X、Y）をXさんからYさんへの通信とするとき、この時の暗号化方式を受信者であるYさんが自由に決定できるようにすればよい。

さらに、XさんからYさんへ送られる情報が、Yさんが事前に決めておいた方式で自動的に暗号化されるようにする。

Yさんが信頼する暗号化技術が、Xさんから見て信頼できる技術であるとは限らない。XさんがYさんから情報を送ってもらう時は、順序対（Y、X）によって決まる暗号化方式、すなわちXさんがYさんに対してしてあらかじめ指定しておいた暗号化方式で暗号化して送信してもらうようにすればよい。

これは、次の各項目を考えれば可能となる。

【０００９】

【アドレス帳の拡張】

現在、インターネットでの通信に利用するソフトにはアドレス帳があり、そこには名前、メールアドレス、組織、電話番号などが記述されている。

これを拡張し、暗号化鍵、暗号化ソフト、復号化鍵、復号化ソフトの４項目を追加する。

たとえば、つぎのように変更する。

秋山氏のアドレス帳

氏名	アドレス	暗号化鍵	暗号化ソフト	復号化鍵	復号化ソフト
X社	Xcp@kabu	ＫＣax	Ｃax	ＫＰxa	Ｐxa
伊藤	Itou@asn	ＫＣai	Ｃai	ＫＰia	Ｐia
斉藤	Saito@uu	ＫＣas	Ｃas	ＫＰsa	Ｐsa
馬場	Baba@yy	ＫＣab	Ｃab	ＫＰba	Ｐba

【００１０】

【通信時におけるソフトウエアの機能】

ＸさんがＹさんに情報を送るとする。このとき、順序対（Ｘ、Ｙ）が決まりこれに対応する暗号化方式をこの順序対に対して一意的に決定できる。この事実をもとにして、次のように機能しなくてはならない。

【００１１】

【送信時の機能】

送信する情報が与えられたら、電子メールの宛先を調べて、アドレス一覧の暗号化鍵、暗号化ソフトの項目をチェックする。それが指定されていたら、暗号化鍵と送信内容を引数として、指定された暗号化ソフトを呼び出し送信する内容を暗号化する。

宛先のアドレスと送信元のアドレスのみを記述した空のメールに、暗号化したものを添付ファイルとして送信する。

もちろん、アドレス帳に記載されていない相手や、アドレス帳に記載されていても暗号化項目が指定されていない場合は暗号化しないでそのままメールを送る。

送信時の機能に関しては、図１を参照してください。

【００１２】

【受信時の機能】

受信時には、発信者のメールアドレスを自分のアドレス帳から探し、その発信者の項目に復号化鍵と復号化ソフトが与えられていたら、復号化鍵と添付ファイルを引数として復号化ソフトを呼び出し、復号化を行う。そして暗号化されていない情報を表示する。

もちろん、アドレス帳に記載されていない相手や、アドレス帳に記載されていても復号化項目が指定されていなければ復号化しないでそのままメールを開く。このような機能をもったソフトウエアまたはハードウエアを作成する。

受信時の機能に関しては、図２を参照してください。

【００１３】

【使用できる暗号の種類と特徴】

暗号には、大きく分けて秘密鍵方式と公開鍵方式の２種類があるがどちらも利用可能である。社会的な評価が高く、専門家が有効と認めるような暗号ソフトの種類は１００種類程度であろう。

暗号化鍵と暗号化ソフトが統一された形で実現されたものは、実用上問題が生じる。それは、暗号化鍵のサイズは１Ｋバイト程度であろうが、統一されたものは１Ｍバイトから１０Ｍバイト程度になる。このサイズのものを１００００人分保存するには１００Ｇバイトが必要になり、１０Ｇバイト程度のハードディスクでは、困難となる。

共通の暗号化ソフトが利用できるならば、暗号化鍵が１００００人分あってもそのサイズは１０Ｍバイト程度ですむ。

理論上は、暗号化鍵と暗号化ソフトを分離しなくても良いのだが、ハードウエアの現状に適しているとの理由で、暗号化鍵と暗号化ソフトを分離する方式で記述しておく。

暗号用の商用ソフトは、次のような構造を持つものとして制作されるのが望ましい。

（１）暗号化鍵の作成機能をもち、鍵の自由な配布が認められている。

（２）暗号化ソフトの自由な再配布が認められている。

（３）復号化鍵の作成機能をもつ。

（４）復号化ソフトの再配布を禁止できる。

この、１から４を満たすようになっていれば秘密鍵方式でも、公開鍵方式でもどちらも利用することができる。このような構造で暗号ソフトを制作することは困難ではない。

復号化ソフトの再配布が禁止できれば、暗号ソフトの利用者がそれぞれにソフト

を購入することになり、商業的にソフトを制作販売することが可能となり、より優れた暗号ソフトの開発が可能となる。

暗号ソフトを自作しても良いが、安全な暗号ソフトを作成するのはかなりの時間と努力を必要とする。暗号ソフトは既にかなりの種類が存在し、日本が世界をリードしている現状があるので、社会的評価の高いものを選ぶのが現実的な選択である。

【００１４】

【秘密鍵方式を使う場合】

秘密鍵方式を使うときは、秘密鍵と暗号化ソフトを事前に配布しておけばよい。

具体例としてシーザー暗号方式の場合を示す。

秋山氏は、シーザー暗号を使うことにし、伊藤氏からの情報は暗号化鍵（－１）で、斉藤氏からの情報は２で暗号化してもらうことにしたとする。

秋山氏のアドレス帳

氏名	アドレス	暗号化鍵	暗号化ソフト	復号化鍵	復号化ソフト
X社	Xcp@kabu	ＫＣax	Cax	２５	P
伊藤	Itou@asn	ＫＣai	Cai	1	P
斉藤	Saito@uu	ＫＣas	Cas	－２	P
馬場	Baba@yy	ＫＣab	Cab	２２	P

秋山氏は、暗号化鍵と暗号化ソフト（Ｃ）を伊藤氏と斉藤氏に送る。伊藤氏、斉藤氏は自分のアドレス帳の暗号化欄に登録する。

伊藤氏、斉藤氏のアドレス帳は次のようになる。

伊藤氏のアドレス帳

氏名	アドレス	暗号化鍵	暗号化ソフト	復号化鍵	復号化ソフト
X社	Xcp@kabu	ＫＣix	Cix	ＫＰxi	Pxi
秋山	Akiyama@ss	（－１）	C	ＫＰai	Pai

斉藤	Saito@uu	ＫＣis	Ｃis	ＫＰsi	Ｐsi
馬場	Baba@yy	ＫＣib	Ｃib	ＫＰbi	Ｐbi

斉藤氏のアドレス帳

氏名	アドレス	暗号化鍵	暗号化ソフト	復号化鍵	復号化ソフト
X社	Xcp@kabu	ＫＣｓx	Ｃｓx	ＫＰxs	Ｐxs
伊藤	Itou@asn	ＫＣsi	Ｃsi	ＫＰis	Ｐis
秋山	Akiyama@ss	2	Ｃ	ＫＰas	Ｐas
馬場	Baba@yy	ＫＣｓb	Ｃｓb	ＫＰbs	Ｐbs

伊藤氏から秋山氏への通信（IBM）は、鍵（－１）で暗号化され、(HAL)となる。
伊藤氏からの暗号文（HAL）は、秋山氏の伊藤氏からの通信に対する鍵（１）で復号化され（IBM）に戻る。
斉藤氏から秋山氏への通信（IBM）は、鍵（２）で暗号化され、（KDO）となる。
暗号文（KDO）は、鍵（－２）で復号化され、（IBM）にもどる。
つまり、暗号化鍵の数だけ文字を先に進め、復号化鍵の示す数だけ元に戻す形になる。

【００１５】

【公開鍵暗号方式を使う場合】

暗号化した情報を送ってもらいたい相手全員に公開鍵を送っておけばよい。また、暗号化ソフトも同じものを配布しておく。もちろん、公開鍵方式にもその実現形態はいろいろあるので、相手ごとに別の公開鍵方式による暗号化ソフトを利用することも可能である。

具体例として、離散対数を利用した場合を示す。

素数p,qを選び、n = pq とする。K = lcm(p-1 , q-1) として、gcd(d,K)=1 となるd を選ぶ。つぎに、ed = 1 (mod K) , ０＜e＜K,となる整数e を計算する。

秋山氏は、e , n を公開し、暗号化ソフト（C）を送付する。

ｄは秘密とし、自分のアドレス帳にnと共に登録しておく。

秋山氏のアドレス帳

氏名	アドレス	暗号化鍵	暗号化ソフト	復号化鍵	復号化ソフト
X社	Xcp@kabu	ＫＣax	Ｃax	d,n	ＰＳ
伊藤	Itou@asn	ＫＣai	Ｃai	d,n	ＰＳ
斉藤	Saito@uu	ＫＣas	Ｃas	d,n	ＰＳ
馬場	Baba@yy	ＫＣab	Ｃab	d,n	ＰＳ

秋山氏は、暗号化鍵と暗号化ソフトを伊藤氏と斉藤氏に送ったとする。
伊藤氏、斉藤氏のアドレス帳は次のようになる。

伊藤氏のアドレス帳

氏名	アドレス	暗号化鍵	暗号化ソフト	復号化鍵	復号化ソフト
X社	Xcp@kabu	ＫＣix	Ｃix	ＫＰxi	Ｐxi
秋山	Akiyama@ss	e, n	Ｃ	ＫＰai	Ｐai
斉藤	Saito@uu	ＫＣis	Ｃis	ＫＰsi	Ｐsi
馬場	Baba@yy	ＫＣib	Ｃib	ＫＰbi	Ｐbi

斉藤氏のアドレス帳

氏名	アドレス	暗号化鍵	暗号化ソフト	復号化鍵	復号化ソフト
X社	Xcp@kabu	ＫＣｓx	Ｃｓx	ＫＰxs	Ｐxs
伊藤	Itou@asn	ＫＣｓI	ＣｓI	ＫＰis	Ｐis
秋山	Akiyama@ss	e , n	Ｃ	ＫＰas	Ｐas
馬場	Baba@yy	ＫＣｓb	Ｃｓb	ＫＰbs	Ｐbs

数　ｘ　を送信するとすれば、
伊藤氏と斉藤氏の持っている暗号化ソフトＣはe,nを使って、
$x^e \equiv c \pmod n$ を計算し、このｃを秋山氏へ送信する。
受け取った秋山氏は $c^d \equiv x \pmod n$ によってｘを得る。すなわち、法ｎでｃの

ｄ乗を計算して、ｘを得る。

【００１６】

【暗号化鍵と暗号化ソフトの配布方法】

情報を送ってもらおうとする相手に、あらかじめ暗号化鍵と暗号化ソフトを所持させる必要がある。直接会ってフロッピーディスクなどに記録したものを渡す。それらを郵送する。又は公開鍵暗号方式などによって暗号化したものを、ネットワークを使って送るなどの方法がある。

【００１７】

【暗号化鍵と暗号化ソフトの登録】

暗号化鍵と暗号化ソフトを受け取った人は、自分のアドレス帳に登録する。

たとえば、秋山氏が伊藤氏との通信で暗号を利用することにしたとする。

順序対（伊藤、秋山）に対応する暗号化方式がきまる。秋山氏が伊藤氏からの通信を受信するときの暗号化方式を Ｃ(i,a) とする。

秋山氏は、伊藤氏に会って、暗号化ソフト（Ｃia）と暗号化鍵（ＫＣia）を手渡す。伊藤氏は、アドレス帳の秋山氏の項目に、この暗号化ソフトと暗号化鍵を登録し、暗号化ソフトと暗号化鍵をハードディスク内に記録しておく。

伊藤氏のアドレス帳は、

氏名	アドレス	暗号化鍵	暗号化ソフト	復号化鍵	復号化ソフト
X社	Xcp@kabu				
秋山	Akiyama@ss	ＫＣia	Ｃia		
斉藤	Saito@uu				
馬場	Baba@yy				

のようになる。

【００１８】

【復号化ソフトの登録】

秋山氏は、伊藤氏からの情報を受信するときに利用する暗号方式を決定したので

、これによって決まる復号化鍵（ＫＰia）と復号化ソフト（Ｐia）を、アドレス帳の伊藤氏の欄にある復号化鍵、復号化ソフトの項目に登録する。

秋山氏のアドレス帳は

氏名	アドレス	暗号化鍵	暗号化ソフト	復号化鍵	復号化ソフト
X社	Xcp@kabu				
伊藤	Itou@asn			ＫＰia	Ｐia
斉藤	Saito@uu				
馬場	Baba@yy				

のようになる。

このアドレス帳により、秋山氏は伊藤氏からの通信を（Ｃia）によって暗号化した形で送ってもらうことができる。また、届いた情報は、（Ｐia）によって自動的に解読される。

秋山氏は、同じ暗号化方式、同じ暗号化鍵を伊藤氏以外の人との通信で利用することもできるし、暗号化方式は同じでも、暗号化鍵は変えて他の人との通信を行うこともできる。

また、全く別の方式で暗号化した通信を行うこともできる。なぜなら、暗号化方式とその実現形態は送信者と受信者の順序対で決まるのだから。

伊藤氏が、秋山氏から送られてくる情報の暗号化に別の方式を選択できることも明らかである。

【００１９】

【復号化ソフト再配布禁止の意義】

暗号化ソフトが、同時に復号化ソフトとして機能することがないようにしておけば、暗号ソフトを購入してこの方式を利用する人は、それぞれ、復号化ソフトを必要とするので、個別に暗号ソフトを購入しなくてはならないことになる。

なぜなら、復号化ソフトは再配布が禁止となっているから。このことは、暗号ソフトの商業的開発を保証し、より安全な通信のための経済的基盤となる。暗号ソフトの開発には長時間の研究が必要であり、経済的保証がなければ優れた暗号ソ

フトを開発することはできない。

【００２０】

【暗号ソフトの名前の一意性】

異なる暗号ソフトに同じ名前が付くと、ハードディスクの中に保存するときに問題が生じる。したがって、暗号ソフトの開発者が持つ一意的な識別記号（メールアドレスなど）をその暗号ソフトの名前に使用して、名前の衝突が起きないようにする必要がある。

【００２１】

【商業的利用】

証券会社（Ｘ社）は、顧客に対して有料での情報提供を行うとする。ある顧客が自動車会社に関心を持っていたとする。その顧客にとっては自動車会社の新車開発情報などは自分だけに知らせてもらえるなら、高い値段が付いていても購入する価値のある情報である。

しかし、この自分だけが知りたい情報の伝達が、ネットワーク上で盗聴や改竄を受けるおそれがあるので、今ひとつ不安がある。

そこで、Ｘ社はこのシステムを採用するとする。

Ｘ社の顧客アドレス一覧は

氏名	顧客アドレス	暗号化鍵	暗号化ソフト	復号化鍵	復号化ソフト
秋山	Akiyama@ss	ＫＣxa	Ｃxa	ＫＰax	Ｐax
伊藤	Itou@asn	ＫＣxi	Ｃxi	ＫＰix	Ｐix
遠藤	Endo@kk	ＫＣxe	Ｃxe	ＫＰex	Ｐex
山田	Yamada@yama	ＫＣxy	Ｃxy	ＫＰyx	Ｐyx

のようになる。

Ｘ社は、顧客の関心を持つ経済分野の情報を有料で配信するとする。顧客が暗号化方式を決定するのが原則であるが、社会的に評価の高い暗号ソフトを１０種類程度は紹介する必要がある。

逆に、顧客からの注文などを受け取るための暗号方式を決定する。これは顧客の

購買力によって方式を変えることもできる。

できれば、異なった暗号化鍵を顧客の数だけ作り出せるものが便利である。しかも、復号化鍵はお客ごとに異なるとしても、復号化ソフトは同じものが利用できるような暗号ソフトがよい。ここにも、復号化鍵と復号化ソフトを分離できる形のメリットが見いだせる。

価値ある経済情報は自分だけに知らせてほしいと思うし、この情報がネットワーク上で盗聴されたり改竄されたりすることを防ぎたいものである。

この方式は、顧客自身の責任で自分のための情報を保護できる。これによって情報にさらなる付加価値を付けることができる。これは、経済的に価値の高い情報を伝えるためには不可欠の方式である。

【００２２】

【個人による利用】

この方式を個人が利用する場合には、アドレス帳は次のような形になる。個人で利用する場合は、経済的負担を考える必要がある。

公開鍵暗号などの場合は、同じ暗号化鍵を配布すればすむので、復号化鍵、復号化ソフトは１種類で済ませることもできる。また、商業的な通信と友人間の通信に分けて、別の公開鍵方式を採用することもできる。

秘密鍵方式では、相手ごとに異なる秘密鍵を作成し、これに対応した復号化鍵を自分のアドレス帳の復号化鍵の欄に記録しておくようにする。鍵が異なっても同じ暗号化ソフト、同じ復号化ソフトを使用することもできるので、ハードディスクなどの資源を節約することもでききる。もちろん、通信相手ごとに暗号化方式を変えても良い。

暗号化ソフトが、暗号化鍵と一体化されていると比較的大きなサイズとなり、これをアドレス帳に記載された人数分だけ自分のハードディスクの中に用意することになる。

人数が増えると、２０Ｇバイト程度のハードディスクでは容量が不足する。そこで、サイズの小さな暗号化鍵は、アドレス帳に記載された人数分だけ用意するにしても、サイズの大きな暗号化ソフトは、共通に利用できることが望ましい。

現実的に有効と認められる暗号ソフトは１００程度と思われる。暗号化ソフトが

共通で利用できるなら、ハードディスクに１００種類だけ置いておけばすむ。また、暗号化ソフトだけを、雑誌の付録などで配布することも可能であるので、実際にはそれを入手し、暗号化鍵だけをやりとりすることも、現実的な方法である。

秋山氏のアドレス帳

氏名	アドレス	暗号化鍵	暗号化ソフト	復号化鍵	復号化ソフト
X社	Xcp@kabu	ＫＣax	Ｃax	ＫＰxa	Ｐxa
伊藤	Itou@asn	ＫＣai	Ｃai	ＫＰia	Ｐia
斉藤	Saito@uu	ＫＣas	Ｃas	ＫＰsa	Ｐsa
馬場	Baba@yy	ＫＣab	Ｃab	ＫＰba	Ｐba

伊藤氏のアドレス帳

氏名	アドレス	暗号化鍵	暗号化ソフト	復号化鍵	復号化ソフト
X社	Xcp@kabu	ＫＣix	Ｃix	ＫＰxi	Ｐxi
秋山	Akiyama@ss	ＫＣia	Ｃia	ＫＰai	Ｐai
斉藤	Saito@uu	ＫＣis	Ｃis	ＫＰsi	Ｐsi
馬場	Baba@yy	ＫＣib	Ｃib	ＫＰbi	Ｐbi

このシステムでの通信用ソフトは次のように機能する。

電子メールを送るときには、宛先のアドレスと、発信者のアドレスが最初に決まり、発信者と受信者の順序対が決まることになる。この順序対に対に対応した暗号化方式によって自動的に暗号化される。

受信者の方では、発信者のアドレスと宛先である自分のアドレスの順序対から復号化方式を決定できるので、暗号化されて送付された情報を自動的に復号する。

たとえば、秋山氏は伊藤氏からの情報を受信するときに利用する暗号化方式を決定する。秋山氏は伊藤氏との通信で使う暗号化鍵（ＫＣia）、暗号化ソフト（Ｃ

ia）、復号化鍵（ＫＰia）、復号化ソフト（Ｐia）を用意し、このうち暗号化鍵（ＫＣia）、暗号化ソフト（Ｃia）に関する情報を事前に伊藤氏に送っておく。伊藤氏はアドレス帳の秋山氏の項目に、暗号化鍵と暗号化ソフトを登録しておく。

伊藤氏から秋山氏へのメールは秋山氏が決めた暗号化方式（Ｃia）と暗号化鍵（ＫＣia）によって暗号化される。これを受け取った秋山氏の通信用ソフトは、送信者のアドレスと、自分のアドレスを判別できるので、これによって復号化方式（Ｐia）と復号化鍵（ＫＰia）を自動的に選びこの方式で復号化する。

逆に、伊藤氏は秋山氏からの情報を受け取るための暗号化方式を決定する。もちろん、この方式は伊藤氏が自由に決定できる。秋山氏からの情報を受け取るために使う暗号化鍵（ＫＣai）、暗号化ソフト（Ｃai）、復号化鍵（ＫＰai）、復号化ソフト（Ｐai）を用意する。このうち、暗号化鍵（ＫＣai）、暗号化ソフト（Ｃai）　を事前に秋山氏に伝えておく。

秋山氏から伊藤氏へのメールは伊藤氏が決めた暗号化方式（Ｃai）と暗号化鍵（ＫＣai）によって暗号化される。受け取った伊藤氏は、秋山氏用の復号化鍵（ＫＰai）と復号化ソフト（Ｐai）を使って解読する。

【００２３】

【暗号方式の更新】

暗号技術の進歩は驚くほど早く、暗号解読技術も同時に進歩している。一つの暗号化方式が安全であるのはせいぜい５年間くらいである。したがって、情報の受信者自身が利用する暗号技術を自由に更新できることが必要である。

この方式では、この変更が情報の受信者の意志で自由にできる。その時点での最も優れた暗号技術を選択することも、利用者の経済的状況が許せば可能となる。

新しい暗号方式を利用すると決めた人は、新しい暗号ソフトを購入し、その暗号化部分を自分のアドレス帳に記載されている人に配布し、その登録を依頼する。また、自分のアドレス帳の復号化部分の登録内容を更新する。

もちろん、簡単な暗号化でよい人や、暗号化が必要ない人もいるだろうが、自分の部屋の鍵を自分で決めるように、自分の意志で、自分の扱う情報の価値にあった暗号化方式を決定できることが重要である。

【００２４】

【機能の拡張】

暗号化、復号化の欄を複数にして複数回の暗号化を重ねることも可能である。特に有料での情報配信では、顧客の決定する暗号方式以外に、最低限の強度を持つ暗号化方式を企業の側で採用し、情報を少なくとも２重に暗号化するべきである。

【００２５】

【電話の場合】

電話でこの方法を利用する場合は、いくつかの通信規格を決定すればよい。

第１は音声をデジタル化するときのサンプリングレートの規格。

第２はデジタル化した音声を一定量ごとに暗号化する時のその量に関する規格。

この２点が決まれば、電話番号が通知される事を利用して、送信者と受信者の電話番号の順序対によって決まる暗号化による秘密通信が電話の場合でも可能となる。

家庭用の電話機の場合は記憶装置と演算装置を組み込むことは簡単であり、電源の問題も心配なく、暗号化と復号化の処理速度の問題だけを解決すればよい。

携帯電話の場合はメモリースティックなどで記憶装置の問題は解決できる。暗号方式を簡単にすれば演算装置の大きさの問題点も解決できる。例えば、データが１０２４ビットごとに暗号化されるとする。暗号化鍵と復号化鍵をこのビット長に相当する文章とし、送信者と受信者で同一の文章を使用する。暗号化方式と復号化方式はXORとする。暗号化も復号化もデジタルデータと鍵となる文章の１０２４ビットごとのXORによって実現できる。文章は記憶装置に書き込んでおけばよい。XORだけなら簡単な回路で実現できるので本格的な演算装置を使う必要はない。残る問題点として、

第３は記憶装置と演算装置を組み込んだ電話機の制作。

である。これは新しい需要を喚起する事になる。このようなコンピュータに近い電話機の制作販売は日本の景気回復にも役立つであろう。携帯電話で使える小型の本格的な演算装置の開発には少し時間がかかるであろう。

【００２６】

【発明の効果】

この秘密通信の方法は、送信者と受信者の順序対ごとの個別的な形での秘密通信を実現する。このときの暗号方式を受信者が自分で決定する事になる。

自分の責任で自分の受信する情報を守ることができる。自分が最も信頼する方式を選択できるので、安心してネットワーク社会に参加できるようになる。

安全な情報を受け取れるので、経済価値の高い情報の受信や発信も安心して行うことができる。有料での情報配信の基礎として有効に機能する。

あくまでも受信者が暗号方式を決定することになるので、自己責任を前提としたネットワーク社会への参加となり、自立的かつ積極的な姿勢でネットワーク社会に参加するようになる。従って、主体的で活発な国際的交流が可能となる。

暗号ソフトの商業的開発や販売がより規模の大きなものとなる。暗号の理論やソフトの作成の面で数学の理論が必要になり数学が役に立つ事を皆が確認できる。日本人の数学の力を情報の安全性向上のために利用でき、それを通じて世界に貢献できる。

また、電話機でこの方式を使うことになれば、電話機そのものを新しく制作する事になり、新たな需要を作り出すことになる。この新しい電話機がすべての家庭に取り付けられれば、日本中の家庭がコンピュータで結ばれているのと同じ事になり、新たなサービスの可能性が無限に広がる。

【図面の簡単な説明】

【図１】　通信用ソフトの送信時の機能を示したもの

【図２】　通信用ソフトの受信時の機能を示したもの

【用語の説明】

１．暗号化部分

平文から暗号文を作るソフトには、暗号化鍵と暗号化ソフトからなるもの、暗号化鍵を使用しないもの、暗号化鍵を暗号化ソフトの中に組み込み一体化させたものなど色々あるが、平文を暗号化する機能を持つ部分を暗号化部分という。

２．復号化部分

暗号文から平文をつくるソフトには、復号化鍵と復号化ソフトからなるもの、復号化鍵を使用しないもの、復号化鍵を復号化ソフトの中に組み込み一体化させたものなど色々あるが、暗号文から平文を復元する機能を持つ部分を復号化部分という。

３．暗号ソフト

暗号通信に使用する暗号化ソフト、暗号化鍵、復号化ソフト、復号化鍵の総体を表す言葉である。

４．シーザー暗号

ローマ時代シーザーが使用したと言われる暗号であり、２６を法とする剰余計算を特徴とする。

５．離散対数

Ｚp上で、$\alpha^{e} \equiv a \pmod{p}$ の関係があるとき、e をa　の離散対数と呼ぶ。

６．XOR

排他的論理和を意味する。

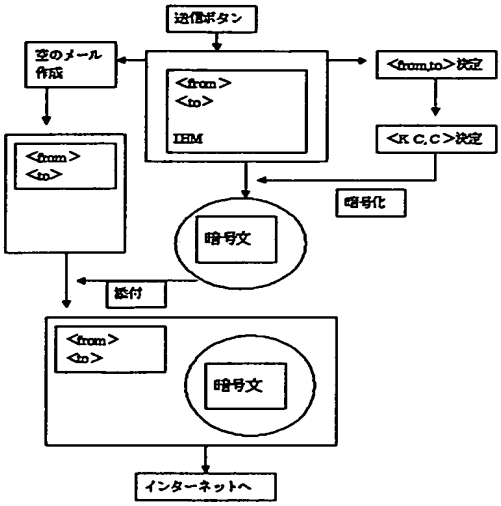
計算は、１XOR１＝０，１XOR０＝１，０XOR１＝１，０XOR０＝０となる。

７．復号化

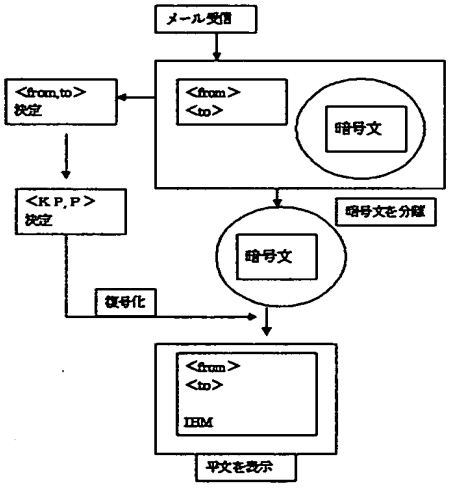
暗号文からもとの平文を復元させること。

【書類名】　　図面

【図１】


送信ボタン
空のメール作成
<from>
<to>
IHM
<from,to>決定
<K C,C>決定
暗号化
暗号文
<from>
<to>
添付
<from>
<to>
暗号文
インターネットへ

【図２】


メール受信
<from,to>
決定
<from>
<to>
暗号文
<K P,P>
決定
暗号文を分離
暗号文
復号化
<from>
<to>
IHM
平文を表示

【書類名】　要約書

【要約】

【課題】　通信の安全性を強化する。

【解決手段】

（１）送信者と受信者の順序対（Ｓ，Ｒ）に対して一意的に決まる暗号方式による秘密通信。

（２）暗号化指定欄と復号化指定欄があるアドレス帳を備え、指定欄の内容に従って自動的　に暗号化と復号化を行う通信ソフト。

（３）暗号化部分と復号化部分に分割でき、暗号化部分の再配布が自由な暗号ソフト。

【効果】　この１，２，３を利用する方法で秘密通信を実現すれば、暗号解読技術の進歩に合わせて新しい理論を利用した信頼度の高い暗号方式に変えてゆくことができ、秘密を保つ必要がある情報でも盗聴や改竄を恐れずにネットワークで提供できる。情報に安心という付加価値を付けた有料の情報提供をすることができる。暗号化部分だけの再配布を認めることで、商業的に暗号ソフトを開発できる。電話でこの方法を採用すれば、新しい電話機に対する需要を掘り起こすことになる。なによりも、各人が主体的にネットワーク社会に参加するようになる。

認定・付加情報

特許出願の番号	特願２０００－３８８９２１
受付番号	５００００１６５２２６８
書類名	特許願
担当官	濱谷　よし子　　１６１４
作成日	平成１２年１２月２６日

＜認定情報・付加情報＞

【提出日】　平成12年12月21日

次頁無

出 願 人 履 歴 情 報

識別番号　　〔３００００８５８６４〕

１．変更年月日　　２０００年１１月１８日
［変更理由］　新規登録
住　所　神奈川県横須賀市久里浜８－３０－１５－５０４
氏　名　宇山　靖政